

METHOD, PROGRAM AND SYSTEM FOR AUTOMATICALLY DETECTING MALICIOUS COMPUTER NETWORK RECONNAISSANCE

ABSTRACT

A detection and response system that generates an Alert if unauthorized
5 scanning is detected on a computer network that includes a look-up table to record
state value corresponding to the sequence in which SYN, SYN/ACK and RST packets
are observed. A set of algorithms executed on a processing engine adjusts the state
value in response to observing the packets. When the state value reaches a
predetermined value indicating that all three packets have been seen, the algorithm
10 generates an Alert.